

Sample: fictional app, not a real client.

FREE CHECK REPORT

# bookings.example.com

<https://bookings.example.com/>

---

|         |                   |
|---------|-------------------|
| Date    | 6 October 2026    |
| Version | 2                 |
| Status  | Reviewed by Aaron |

## Summary

Two things need fixing this week: a live Stripe secret key in the JavaScript every visitor downloads, and public source maps that hand out the app's original code. The rest fits into a normal sprint. One automated finding was removed in review: the Google Maps key in the bundle is restricted to this domain, as it should be.

## Findings by severity

| Critical | High | Medium | Low | Info | Total |
|----------|------|--------|-----|------|-------|
| 1        | 1    | 3      | 2   | 0    | 7     |

## Findings ranked by business impact

In the order they matter to the business. Each is set out in full in the next section.

| # | Finding                                                                            | Severity | Effort |
|---|------------------------------------------------------------------------------------|----------|--------|
| 1 | <b>Live Stripe secret key in the shipped JavaScript</b><br>Security exposure       | Critical | Hours  |
| 2 | <b>JavaScript sourcemaps are public</b><br>Security exposure                       | High     | Hours  |
| 3 | <b>Customer email addresses in confirmation page URLs</b><br>Security exposure     | Medium   | Hours  |
| 4 | <b>Error pages show a stack trace</b><br>Security exposure                         | Medium   | Hours  |
| 5 | <b>No Strict-Transport-Security header</b><br>Fundraising and enterprise sales     | Medium   | Hours  |
| 6 | <b>1.9 MB of JavaScript before the first screen</b><br>Revenue                     | Low      | Days   |
| 7 | <b>X-Powered-By header names the framework</b><br>Fundraising and enterprise sales | Low      | Hours  |

## Detailed findings

### **Critical** Live Stripe secret key in the shipped JavaScript

Business impact · Security exposure

Anyone who opens the booking page can use this key to issue refunds, create charges or read your customers' payment records.

Recommended fix

Roll the key in the Stripe dashboard today, then move the deposit and refund calls into server-side code so the key never reaches the browser.

Effort

Hours

Evidence

- `/assets/index-3e7a19c0.js: sk_live_...FAKE (107 chars)`

### **High** JavaScript sourcemaps are public

Business impact · Security exposure

The app's original source, including the staff screens and the deposit logic, can be downloaded and read by anyone, which makes the app cheaper to copy and to attack.

Recommended fix

Turn off production sourcemaps in the build (Vite: `build.sourcemap false`), or upload them to the error tracker only, then redeploy.

Effort

Hours

Evidence

- `/assets/index-3e7a19c0.js.map: served: 200, application/json, 3,412,880 bytes; source map shape`

**Medium** Customer email addresses in confirmation page URLs

Business impact · Security exposure

The booking confirmation puts the customer's email address in the page address, where analytics tools and any site the page links to can record it.

Recommended fix

Use the booking ID alone in the confirmation URL and look the email up on the server, then send Referrer-Policy: strict-origin-when-cross-origin.

Effort

Hours

Evidence

- `/assets/index-3e7a19c0.js`: the confirmation route builds `/booking/confirmed?email=...`

**Medium** Error pages show a stack trace

Business impact · Security exposure

A mistyped address shows file paths, library versions and internal structure, which shortens the work of anyone probing the app.

Recommended fix

Turn off debug error pages in production and log the details server-side instead.

Effort

Hours

Evidence

- `/.git/HEAD`: not served, but the 500 error page carries a stack trace with file paths

**Medium** No Strict-Transport-Security header

Business impact · Fundraising and enterprise sales

Enterprise security questionnaires ask for HSTS, so its absence is an easy point to lose in a vendor review, and a first visit over plain http can be intercepted.

Recommended fix

Add Strict-Transport-Security: max-age=31536000; includeSubDomains in the hosting platform's headers configuration.

Effort

Hours

Evidence

- `https://bookings.example.com/`: header absent on the root response

Low

**1.9 MB of JavaScript before the first screen**

Business impact · Revenue

On a mid-range phone the booking page takes several seconds to appear, which costs bookings from paid traffic.

Recommended fix

Split the staff screens and the calendar library into lazily loaded routes so the booking page ships only what it draws.

Effort

Days

Evidence

- `/`: 5 scripts, 1,992,431 bytes decoded

Low

**X-Powered-By header names the framework**

Business impact · Fundraising and enterprise sales

The header tells anyone which framework runs the app, which shortens the search for a known weakness.

Recommended fix

Remove the X-Powered-By header (in Express: `app.disable('x-powered-by')`).

Effort

Hours

Evidence

- `https://bookings.example.com/`: X-Powered-By: Express

## Not assessed

- **Data access:** Data-access probes are not enabled

## Next step

This free check looked only at what the deployed app shows the public internet. The paid audit reviews the code itself, and the product and business goals behind it, and ends with a fixed-price plan to fix what matters.

Book the audit: <https://anyfront.co/book>

---

A professional review of the stated scope at the stated time. Not a security guarantee, penetration test or certification.